

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

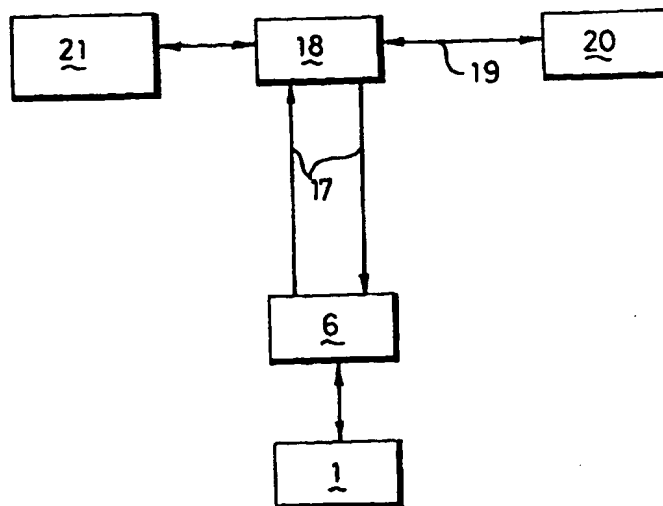


BG

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : G07F 7/10		A1	(11) International Publication Number: WO 99/00775
			(43) International Publication Date: 7 January 1999 (07.01.99)
(21) International Application Number: PCT/GB98/01865			(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).
(22) International Filing Date: 26 June 1998 (26.06.98)			
(30) Priority Data: 9713743.4 27 June 1997 (27.06.97) GB			
(71) Applicant (for all designated States except US): NATIONAL WESTMINSTER BANK PLC [GB/GB]; 41 Lothbury, London EC2P 2BP (GB).			
(72) Inventors; and (75) Inventors/Applicants (for US only): VINER, John, Charles [GB/GB]; 'Hydes', Woodlands Lane, Wyndlesham, Surrey GU20 6AN (GB). EVERETT, David, Barrington [GB/GB]; 31 Ashdown Avenue, Brighton, East Sussex BN2 8AH (GB).			
(74) Agent: BOYDELL, John, Christopher; Stevens, Hewlett & Perkins, 1 Serjeants' Inn, Fleet Street, London EC4Y 1LL (GB).			Published With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: PAYMENT PROCESS AND SYSTEM



(57) Abstract

A payment process and system using a smart card (1) which accesses a remote account at a card issuer (20) via an acquirer (18). The card is read in a terminal (6) which is in two-way communication (17) with the acquirer (18). As part of the payment process, a cryptogram of the transaction data is made by the smart card and used in the terminal (6) as a key to encrypt the PIN, entered by the cardholder, for transmission to the acquirer (18). The acquirer also creates a cryptogram, using the transaction data sent to it by the terminal (6), and uses this cryptogram (which should be the same as that created by the smart card) to decrypt the encrypted PIN. In this way, the use of an expensive tamper-resistant encrypting PIN pad at the terminal (6) is avoided, whilst maintaining security.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

"PAYMENT PROCESS AND SYSTEM"

This invention relates to a payment process and system particularly intended for use with financial transactions involving integrated circuit cards (ICC's), or "smart cards".

As part of a financial transaction involving a credit card or a debit card, it is normally necessary that details of the transaction be communicated to the card issuer or other equivalent body for authorisation of the transaction. Where the credit card or debit card takes the form of a smart card, the card will hold in its memory application software which is activated to carry out the credit card or debit card function, as appropriate. One card may hold both credit card and debit card applications, as well as other financial functions, such as cash cards, or even non-financial functions. The present invention is concerned primarily with the use of smart cards as debit and/or credit cards.

The major card issuers Europay, MasterCard and Visa have jointly developed standards (known as the EMV ICC Specifications for Payment Systems) for smart card based payment systems. Systems developed to these standards enable a card holder to pay for goods and services by accessing a remote account at a bank or other financial institution. As part of such a payment process, the card holder may authenticate himself to the financial institution by entry of a PIN (personal identification number). Where this form of card holder authentication is used then a critical aspect of the system design is ensuring the secure transport of the PIN to the account holding institution.

Access to the remote account is achieved via a terminal into which the user inserts his or her card, usually at the start of the transaction. The terminal is coupled, or able to be coupled, in some way to the account holding institution so that messages can be exchanged between the two. It is very attractive if the terminal used for managing the transaction with the smart card can be a low cost device which would, for example be suitable for home use. EMV compliant applications are not well suited to this

purpose. They are intended as part of a large infrastructure based round terminals with tamper resistant encrypting PIN pads. It is thus not appropriate to use the EMV standards in a normal way to fulfil the requirements for a payment application on a smart card.

5 Despite its unsuitability for the payment application for the purpose explained above, EMV compliant applications do have many of the required attributes, are well understood in the financial community, have been implemented, and have stable associated standards. There are significant benefits if a way can be found of using such applications, without
10 in any way introducing non-EMV compatible commands. The principle object of the present invention is thus to find a way of encrypting the PIN, without incurring the expense of a tamper resistant encrypting PIN pad at the terminal. PIN encryption is not a standard EMV function, as this function is assumed to be carried out by the PIN pad at the terminal.

15 This patent application seeks to provide a payment process and system capable of achieving the above object. A knowledge of the operation of the EMV standards as defined in the document "EMV'96 Integrated Circuit Card Specification for Payment Systems" Version 3.0 dated 30 June 1996 is advantageous for a full understanding of the present
20 invention. However, although the EMV standard and EMV-compliant applications are referenced throughout, the technique is, in principle, applicable to any smart card oriented payment system with similar commands. It is intended that this patent application covers all such implementations; EMV is used, as an example only, to clarify the
25 technique.

 According to a first aspect of the invention there is provided a payment process enabling secure communication between a smart card and a financial institution, said process comprising placing the card in a card reader forming part of a terminal in communication with said financial
30 institution, entering details of the transaction and a PIN into a keypad, creating a cryptogram of transaction data, including said transaction details, using a first cryptographic key known to or derivable by the financial

institution, thence using said cryptogram to encrypt the PIN for secure onward transmission to the financial institution.

The financial institution may be the card issuer, holding the account which corresponds with the card, or more likely will be an intermediary, commonly known as an acquirer, which acts as a link between the terminal and the card issuer. Very likely the acquirer will act as agent for a number of card issuers and is thus responsible for ensuring that messages originating in any one particular issuer's card are properly routed to that issuer.

The terminal is typically situated at a retail premises to enable the cardholder to purchase goods, using the card as a debit or credit card. To this end, the card is pre-loaded with an application program which enables it to function as required. This application is associated with a second cryptographic key, referred to herein as the card key, which card key is downloaded to the card at the same time as the original application, and is known to the financial institution.

The card key may be the same key as the first key, but preferably the cryptographic key used to create the cryptogram (i.e. the first key) is derived from the card key by taking a function of a transaction parameter, conveniently the transaction sequence number, encrypted by the card key. The transaction sequence number is any number which uniquely identifies the transaction. Conveniently, the transaction number is stored in the card and is sequenced by 1 at the start of each new transaction. The transaction number is transmitted to the financial institution as part of the payment process so that, if necessary, the financial institution is able to derive the cryptographic key used to create the cryptogram.

The PIN is decrypted by the financial institution following transmission of the encrypted PIN to the institution. In a preferred embodiment of the invention, this process is carried out by mirroring, at the financial institution, the creation of the cryptogram from the transaction data transmitted to it from the terminal. For this purpose, the financial institution

needs to know, or be able to derive the aforesaid first key. The cryptogram thus created should thus be identical to that created at the card.

By transaction data is meant data relating to the transaction and includes some information entered at the keypad, such as the amount
5 of the transaction, and some information generated internally by the terminal, such as the transaction date (it being assumed that the terminal has a built-in calendar). A cryptogram is, in effect, a digest or summary of the transaction data. In the DES encryption system such cryptograms are sometimes referred to as Message Authentication Codes, or MAC's. The
10 techniques for creating such cryptograms are known in the art. Briefly, the transaction data is divided into small units, for example of 8 bits length, and the units operated on one at a time, starting, for example, at the beginning. Each unit is thus encrypted, using the same key and the same function, with the encrypted output of each unit being added to the next prior to
15 encryption. When all the units making up the transaction data have been cycled through, the resultant output will be derived from all of the units; any change, accidental or otherwise, in the transaction data during transmission will result in the generation of a cryptogram which is different from the first so the fact that a change has been made can be detected.

20 Preferably the cryptogram is used, in effect, as a cryptographic key to encrypt the PIN for onward transmission. In theory several encryption methods can be used; however, this is subject to the important caveat that, whatever method is used, it is not possible for an eavesdropper to reconstruct the PIN and cryptogram separately. In the
25 preferred embodiment the PIN and the cryptogram form respective inputs to an exclusive OR operation which produces code from which neither of the constituent parts can be derived without knowledge of the other. At the financial institution the cryptogram is re-created as mentioned above and therefore, assuming no transmission faults, the PIN can be derived.
30 Whether the PIN is correct for the account held by the issuer is still not, of course, known at this time. Once the PIN has been checked as correct, however, the transaction can proceed.

According to a second aspect of the invention there is provided a payment system for enabling secure communication between a smart card and a financial institution, said system comprising a terminal having a card reader for reading said smart card, and a keypad for enabling
5 entry of transaction details, said card being programmable to create, from transaction data including transaction details entered at the keypad, a cryptogram using a cryptographic key known to or derivable by said financial institution, said terminal further comprising means for using said cryptogram to encrypt a PIN entered at the keypad and means for
10 transmitting the encrypted PIN to the financial institution.

In order that the invention may be better understood, an embodiment thereof will now be described by way of example only and with reference to the accompanying drawings in which:

Figure 1 is a schematic diagram of a smart card for use in a
15 payment process and system according to the invention;

Figure 2 is a block diagram of a payment terminal suitable for use in the payment process and system according to the invention; and

Figure 3 is a block diagram showing a generic system for remote payments using a smart card.

Referring firstly to Figure 1 there is shown a smart card 1
20 having on one surface a contact pad 2 carrying several separate electrical contacts whereby an external power source may be connected to power the card and a serial communication channel may be established to transmit messages and data to and from the card. The card further
25 comprises a microprocessor 3, a non-volatile memory 4, such as ROM (read-only memory) or EEPROM (electrically erasable programmable read-only memory), and a random access memory 5.

The memory 4 holds one or more applications, which define the function of the card, and their associated cryptographic keys. An
30 application is simply a program with associated data files and may, for example, be such as to give the card the functionality of a debit card or a credit card, or both.

In order to use the card in a payment system, it is inserted into a card reader forming part of a payment terminal which can communicate with the card holder's account at a remote location. A simplified block diagram of a suitable payment terminal 6 is illustrated in
5 Figure 2.

Referring to Figure 2, the terminal 6 comprises a microprocessor 7 having non-volatile memory 8, such as ROM or EEPROM, random access memory 9 and, optionally, a display 10 connected via interface circuitry 11. User input is via a keypad 12
10 connected to the microprocessor through interface circuitry 13. The aforementioned card reader is shown under reference 14 and makes contact with the card via the contact pad 2. A communications circuit 15 is provided to enable the terminal to establish two-way communication with the rest of the system, either on a permanent or as-needed basis, via an
15 input/output port 16.

Operation of the terminal 6 is primarily under the control of the microprocessor 7 and its associated circuitry, much of which is not shown for simplicity, but which is well known to those skilled in the art. The terminal forms part of a smart card payment system shown in block
20 diagram form in Figure 3.

In Figure 3, the terminal 6 is shown connected, via a two way communication channel 17, to an acquirer 18. The acquirer is the body which is responsible for managing the overall payment transaction and will probably act as an agent for several card issuers. The acquirer might, for
25 example, be a bank or other financial institution.

The acquirer is connected via a two-way communication channel 19 to a card issuer 20 who, for the purposes of the present explanation, is assumed to be the body who issued the card 6 and who holds the card holder's account. The acquirer 18 is responsible for routing
30 messages from the terminal 6 to the appropriate card issuer for payment authorisation. However, as will be explained below, it is possible for the terminal 6 to communicate directly with the card issuer, thus bypassing the

acquirer; it is even possible, in the simplest system, for there to be no acquirer at all.

Configuration of the card 6 is carried out by a personalisation service (Pserv) 21 which is, in effect, part of the acquirer, but could be part of the card issuer (see below). Configuration of the card is realised by
5 preparing an instance of an application - namely code, associated data, and a cryptographic key - and downloading that instance and key to the card. The application and its associated cryptographic key is thence stored in the card's non-volatile memory 4, as discussed above. Configuration is
10 carried out on new cards, before they can be used, or may be carried out on existing cards in order to update or add functionality to the card. The cryptographic key, referred to hereafter as the card key is used with a cryptographic system to ensure secure transmission of data to and from the card. In payment systems of the type discussed herein, a symmetric
15 cryptographic system, such as the DES system, is conventionally used. This uses a secret cryptographic key, known only to the card 6 and the acquirer 18 to enable encryption and decryption of data sent between the two. In practice, the card key is a function of cardholder identification data, such as account number, encrypted with the master key of the acquirer.
20 The card key is thus unique to the card and can be derived by the acquirer from the cardholder's identity and the master key held by the acquirer.

As part of the payment transaction, the user types his PIN into the keypad on the terminal 6. If the normal type of tamper resistant encrypting PIN pad is in use, the PIN will be encrypted, using a
25 cryptographic "terminal" key known only to the terminal and the acquirer. Meanwhile, the transaction data, including such details as the date and amount of the transaction, is passed to the card, and a cryptogram is created from this transaction data within the card itself, using a
cryptographic transaction key to form a cryptogram. Once created, the
30 cryptogram is returned to the terminal 6. In an EMV-compliant application this cryptogram would be prepared by the card upon receiving a "Generate Application Cryptogram" command which is issued by the terminal. Details

of this EMV command, including its operation and parameters, are given in the EMV specification referred to above. In practice the transaction data is passed as a parameter of the "Generate Application Cryptogram" command which is issued by the terminal and the cryptogram is passed
5 back to the terminal as a return parameter of the command.

The transaction key used to create the cryptogram is derived in the card as a function of a transaction sequence number (which is different for each transaction) encrypted with the card key. The transaction sequence number is likewise passed back to the terminal as a return
10 parameter of the "Generate Application Cryptogram" command.

The cryptogram is next forwarded, together with the transaction data and encrypted PIN, to the acquirer 18. The acquirer checks the transaction data against the cryptogram, decrypts the PIN and then re-encrypts the PIN for onward transmission, with the transaction data,
15 to the appropriate issuer 20. The key used to re-encrypt the PIN is one known to the authorising issuer.

The cryptogram is, in effect an encrypted digest of the transaction data and is such that any tampering with the data, either deliberate or accidental, can be detected by the acquirer or issuer by
20 comparing the received transaction data with its cryptogram. The transaction data will usually be quite long whereas the encrypted digest, or cryptogram, will be much shorter, typically only 8 bits. The manner in which the cryptogram is prepared is well-known in the art and will not be described further.

25 Once the transaction data and re-encrypted PIN arrives at the issuer 20 the issuer checks the PIN supplied by the cardholder and, if correct, checks that the account is in funds, or that any credit limit is not exceeded, and then returns a message authorising the transaction back to the terminal 6, via the acquirer 18.

30 For the purpose of the present invention, it is assumed that the key pad in terminal 8 is not capable of encryption or, if it is, the encryption is not being used. In accordance with an embodiment of the

invention PIN encryption is performed by the terminal after receiving the cryptogram back from the card by using the cryptogram as a cryptographic key. Thus the microprocessor 7 and its associated circuitry derives a function of the PIN encrypted with the cryptogram. An example of a simple
5 logic function which will achieve this is the exclusive OR function. In other words, PIN encryption is performed by creating, in the terminal circuitry, the exclusive OR of the cryptogram and PIN, and it is this data item which is transmitted to the acquirer 18, together with the transaction data, as before. At the acquirer 18 the PIN needs to be decrypted. To do this, the acquirer
10 essentially recreates the cryptogram from the transaction data which it has received from the terminal. It then uses this cryptogram to decrypt the PIN. The PIN is now re-encrypted, using a key known between acquirer and issuer, and is sent to the issuer, for checking of the PIN. Reencryption can be carried out at the acquirer within the confines of a tamper resistant
15 device so that the PIN never appears "in clear" outside the cryptographic domains established between the terminal 6 and issuer 20. If the PIN is correct, the transaction data is interrogated and the appropriate account checked. If all is well, an appropriate authorisation message is passed back to the terminal 6. If the PIN does not check out at the issuer, this may
20 mean that the PIN was not correctly entered at the keypad by the cardholder, or it may mean that the transaction data was corrupted in some way in its passage to the acquirer. Either way, the transaction proceeds no further.

In theory several methods can be used for encrypting the
25 PIN, using the cryptogram as a key. In practice however many possible methods are excluded because the data item which is transmitted from the terminal 6 to the acquirer 18 must not allow for an eavesdropper to reconstruct the PIN and cryptogram separately.

It will be seen that the above-described techniques enable the
30 PIN to be encrypted without using an encrypting PIN pad and in a way which is transparent to the EMV application on the card. Thus the terminal 6 makes the payment transaction appear to the EMV-compliant application

on the card as a standard EMV payment transaction. The present invention makes this approach possible by providing a way of encrypting the PIN for transmission to the issuer, via the acquirer, so that its confidentiality is totally assured in transit. No existing EMV-compliant application function does this because, as mentioned above, PINs are
5 conventionally encrypted by the terminal, not the card.

So far it has been assumed that the personalisation service (PServ) 21 is associated with the acquirer 18. However, the techniques which are the subject of this patent application are equally applicable when
10 PServ 21 is associated with the issuer 20. In this case the encrypted PIN message would pass through the acquirer without any translation. Indeed it would not be possible for the acquirer to decrypt the PIN message as only the application on the card 6 and the issuer 20 would have the requisite keying relationship. If it is important for current standard payment
15 authorisation message formats to be maintained, then a simple issuer based conversion utility could front end the issuer authorisation systems.

In this alternative model the personalisation service PServ could either be issuer specific, or could be supported by a service provider on behalf of several issuers.

CLAIMS

1. A payment process enabling secure communication between a smart card and a financial institution, said process comprising placing the
5 card in a card reader forming part of a terminal in communication with said financial institution, entering details of the transaction and a PIN into a keypad, creating a cryptogram of transaction data, including said transaction details, using a first cryptographic key known to or derivable by the financial institution, thence using said cryptogram to encrypt the PIN for
10 secure onward transmission to the financial institution.
2. A payment process according to claim 1 wherein said card stores a second cryptographic key associated with the card and known to the financial institution, and wherein the first cryptographic key is created during the payment process by encrypting a parameter of the transaction
15 which is unique to the payment transaction in process, using the second cryptographic key.
3. A payment process as claimed in claim 2 wherein the transaction parameter is a transaction sequence number, which is a number which identifies the transaction and is automatically sequenced
20 between transactions.
4. A payment process as claimed in any one of claims 1, 2 or 3 wherein the PIN is encrypted using the cryptogram as a cryptographic key.
5. A payment process as claimed in claim 4 wherein encryption of the PIN is performed by creating the exclusive OR of the cryptogram and
25 the PIN.
6. A payment process as claimed in any one of the preceding claims wherein the cryptogram is created within the card following receipt of a command from the terminal.
7. A payment process as claimed in claim 6 wherein the
30 transaction data is passed to the card as a parameter of the command, and the cryptogram is returned to the terminal as a return parameter of the command.

8. A payment process as claimed in either one of claims 6 or 7 wherein the smart card holds at least one application program which gives the card its functionality, and wherein said applications program is EMV-compatible.

5 9. A payment process as claimed in any one of the preceding claims wherein the encrypted PIN is decrypted at the financial institution by transmitting, with the encrypted PIN, said transaction data, creating in said financial institution a cryptogram of the transmitted transaction data using said first cryptographic key and decrypting the PIN using the just-created
10 cryptogram.

10. A payment process as claimed in claims 2 and 9 wherein, prior to creation of the cryptogram in the financial institution, said first cryptographic key is derived by decrypting the transaction number using the second cryptographic key.

15 11. A payment system for enabling secure communication between a smart card and a financial institution, said system comprising a terminal having a card reader for reading said smart card, and a keypad for enabling entry of transaction details, said card being programmable to create, from transaction data including transaction details entered at the
20 keypad, a cryptogram using a cryptographic key known to or derivable by said financial institution, said terminal further comprising means for using said cryptogram to encrypt a PIN entered at the keypad and means for transmitting the encrypted PIN to the financial institution.

12. A payment system as claimed in claim 11 wherein the
25 financial institution includes means for creating a cryptogram of the transaction data, transmitted from the terminal with the encrypted PIN, using said first cryptographic key.

13. A payment system as claimed in claim 12 wherein said financial institution further comprises means for deriving said first
30 cryptographic key by decrypting the transaction number using the second cryptographic key.

Fig.1.

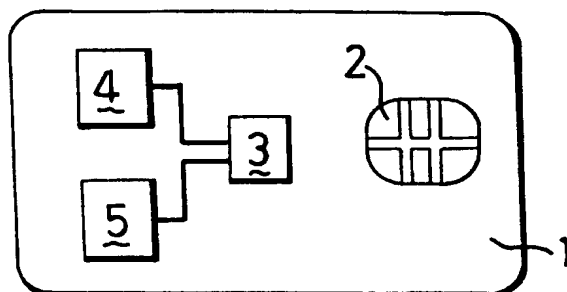


Fig.2.

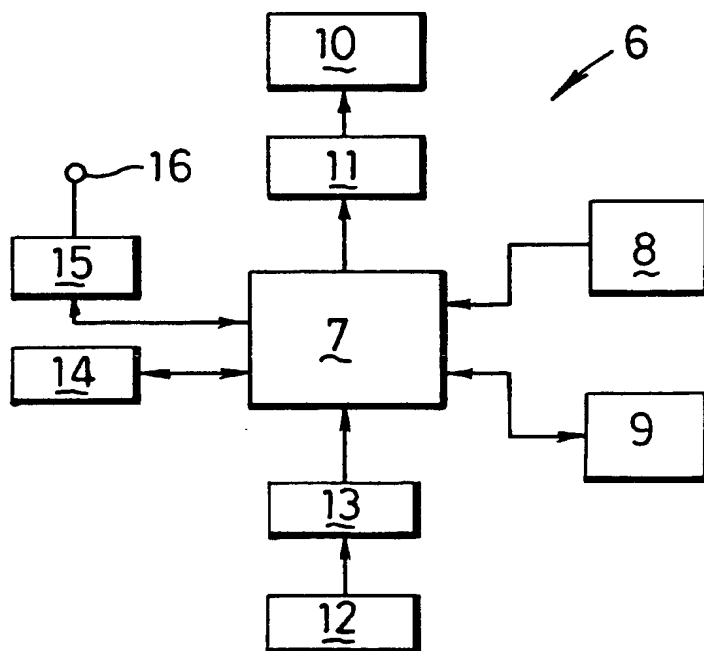
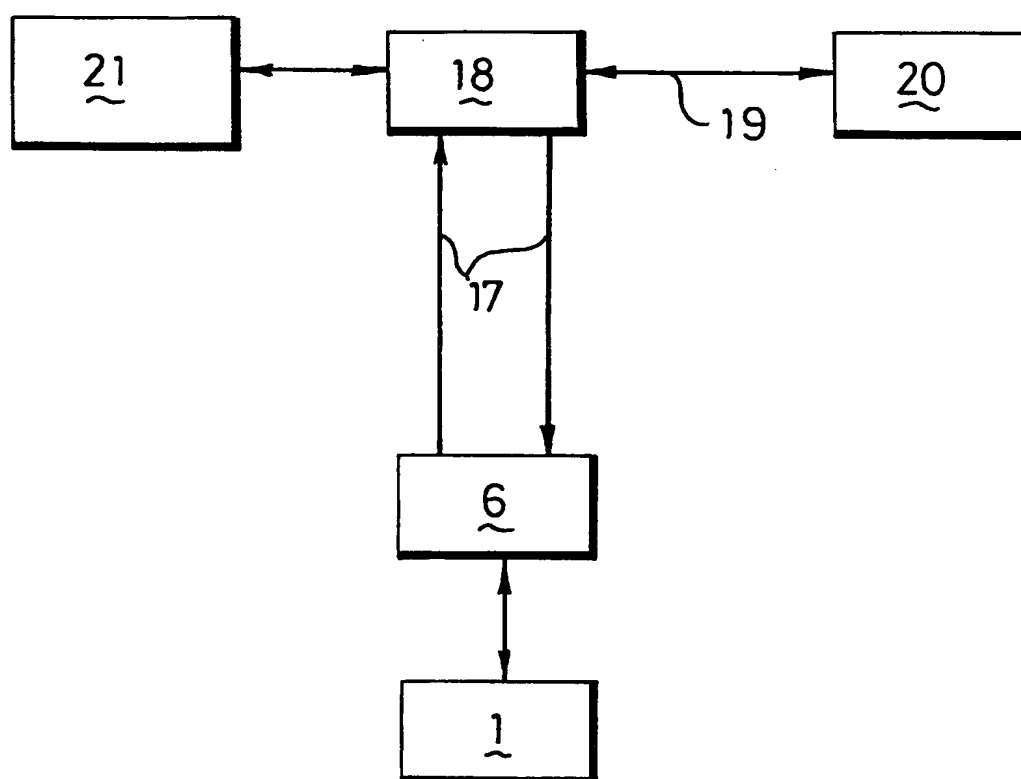


Fig.3.



INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 98/01865

A. CLASSIFICATION OF SUBJECT MATTER G 07 F 7/10		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G 07 F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0385400 A2 (ATALLA CORP.) 05 September 1990 (05.09.90), claims 1,2,5, fig. 3,4. --	1,5,9, 11
A	WO 97/18537 A1 (KONINKLIJKE PTT NEDERLAND N.V.) 22 May 1997 (22.05.97), claims 1,5,17, fig. 1. --	1,6,7, 8
A	EP 0198384 A2 (SIEMENS AG) 22 October 1986 (22.10.86), claims 1,7, fig. 1,2. ----	1,2, 10,12, 13
<input type="checkbox"/> Further documents are listed in the continuation of box C. <input type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>*A* document defining the general state of the art which is not considered to be of particular relevance</p> <p>*E* earlier document but published on or after the international filing date</p> <p>*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>*O* document referring to an oral disclosure, use, exhibition or other means</p> <p>*P* document published prior to the international filing date but later than the priority date claimed</p> </div> <div style="width: 45%;"> <p>*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>* & * document member of the same patent family</p> </div> </div>		
Date of the actual completion of the international search <div style="text-align: center; font-size: 1.2em;">21 September 1998</div>		Date of mailing of the international search report <div style="text-align: center; font-size: 1.2em;">30.10.98</div>
Name and mailing address of the ISA European Patent Office, P.O. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tlx. 31 651 epo nl, Fax (+ 31-70) 340-3016		Authorized officer <div style="text-align: center; font-size: 1.2em;">BISTRICH e.h.</div>

ANHANG

zum internationalen Recherchen-
bericht über die internationale
Patentanmeldung Nr.

ANNEX

to the International Search
Report to the International Patent
Application No.

ANNEXE

au rapport de recherche inter-
national relatif à la demande de brevet
international n°

PCT/GB 98/01865 SAE 199273

In diesem Anhang sind die Mitglieder
der Patentfamilien der in obenge-
nannten internationalen Recherchenbericht
angeführten Patentdokumente angegeben.
Diese Angaben dienen nur zur Unter-
richtung und erfolgen ohne Gewähr.

This Annex lists the patent family
members relating to the patent documents
cited in the above-mentioned inter-
national search report. The Office is
in no way liable for these particulars
which are given merely for the purpose
of information.

La présente annexe indique les
membres de la famille de brevets
relatifs aux documents de brevets cités
dans le rapport de recherche inter-
national visée ci-dessus. Les renseigne-
ments fournis sont donnés à titre indica-
tif et n'engagent pas la responsabilité
de l'Office.

In Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
EP A2 385400	05-09-90	AU A1 50527/90 AU B2 615832 CA AA 2010345 DE CO 69019037 DE I2 69019037 EP A3 385400 EP B1 385400 JP A2 3067355 US A 4965568	06-09-90 10-10-91 01-09-90 08-06-95 12-10-95 26-06-91 03-05-95 22-03-91 23-10-90
WO A1 9718537	22-05-97	AU A1 76255/96 NL A1 1004536 NL C2 1001659 NL C2 1004536 NO A0 982203 NO A 982203	05-06-97 21-05-97 21-05-97 21-05-97 14-05-98 14-07-98
EP A2 198384	22-10-86	EP A3 198384	23-03-88